Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Georges GRAS

On the order modulo p of an algebraic number

Tome 30, nº 1 (2018), p. 307-329.

<http://jtnb.cedram.org/item?id=JTNB_2018__30_1_307_0>

Journal de Théorie des Nombres
de Bordeaux **30** (2018), 307–329

On the order modulo p of an algebraic number

par Georges GRAS

Résumé. Soit $K/\mathbb{Q}$ Galoisienne, et soit $\eta \in K^\times$ de conjugués multiplicativement indépendants. Pour un premier p, non ramifié, étranger à η, soient n_p le degré résiduel de p et g_p le nombre de $\mathfrak{p}|p$, puis $o_\mathfrak{p}(\eta)$ et $o_p(\eta)$ les ordres de η modulo $\mathfrak{p}$ et p respectivement. En utilisant les automorphismes de Frobenius, nous montrons que pour tout $p \gg 0$, certains diviseurs explicites de $p^{n_p}-1$ ne peuvent réaliser ni $o_\mathfrak{p}(\eta)$ ni $o_p(\eta)$, et nous donnons une borne inférieure de $o_p(\eta)$. Ensuite nous obtenons que $\mathrm{Prob}(o_p(\eta) < p) \leq \frac{1}{p^{g_p\,(n_p-1)-\varepsilon}}$, où $\varepsilon = O\big(\frac{1}{\log_2(p)}\big)$, pour tout $p \gg 0$ tel que $n_p > 1$; sous l'heuristique de Borel–Cantelli, ceci conduit à $o_p(\eta) > p$ pour tout $p \gg 0$ tel que $g_p(n_p-1) \geq 2$, ce qui couvre les cas “limites” des corps cubiques avec $n_p = 3$ et des corps quartiques avec $n_p = g_p = 2$, mais non celui des corps quadratiques avec $n_p = 2$. Dans le cas quadratique, la conjecture naturelle est, au contraire, que $o_p(\eta) < p$ pour une infinité de p inertes. Des calculs sont donnés via des programmes PARI.

Abstract. Let $K/\mathbb{Q}$ be Galois, and let $\eta \in K^\times$ whose conjugates are multiplicatively independent. For a prime p, unramified, prime to η, let n_p be the residue degree of p and g_p the number of $\mathfrak{p}|p$, then let $o_\mathfrak{p}(\eta)$ and $o_p(\eta)$ be the orders of η modulo $\mathfrak{p}$ and p, respectively. Using Frobenius automorphisms, we show that for all $p \gg 0$, some explicit divisors of $p^{n_p}-1$ cannot realize $o_\mathfrak{p}(\eta)$ nor $o_p(\eta)$, and we give a lower bound of $o_p(\eta)$. Then we obtain that, for all $p \gg 0$ such that $n_p > 1$, $\mathrm{Prob}(o_p(\eta) < p) \leq \frac{1}{p^{g_p\,(n_p-1)-\varepsilon}}$, where $\varepsilon = O\big(\frac{1}{\log_2(p)}\big)$; under the Borel–Cantelli heuristic, this leads to $o_p(\eta) > p$ for all $p \gg 0$ such that $g_p(n_p-1) \geq 2$, which covers the “limit” cases of cubic fields with $n_p = 3$ and quartic fields with $n_p = g_p = 2$, but not the case of quadratic fields with $n_p = 2$. In the quadratic case, the natural conjecture is, on the contrary, that $o_p(\eta) < p$ for infinitely many inert p. Some computations are given with PARI programs.

Manuscrit reçu le 30 juin 2016, révisé le 21 novembre 2016, accepté le 3 février 2017.
2010 *Mathematics Subject Classification.* 11R04, 11R16.
Mots-clefs. algebraic numbers, order modulo p, Frobenius automorphisms, probabilistic number theory.

1. Frobenius automorphisms

1.1. Generalities. Let $K/\mathbb{Q}$ be Galois of degree n, of Galois group G. Denote by h a possible residue degree of an unramified prime ideal of K, that is to say a divisor of n for which there exists a *cyclic* subgroup H of G of order h. Indeed, one knows that, for any generator s of H, there exist infinitely many prime numbers p, unramified in $K/\mathbb{Q}$, such that s is the Frobenius $s_{\mathfrak{p}}$ of a prime ideal $\mathfrak{p} \mid p$ in $K/\mathbb{Q}$; H is then the decomposition group $H_{\mathfrak{p}}$ of $\mathfrak{p}$. Reciprocally, any unramified $\mathfrak{p}$ has a cyclic decomposition group $H_{\mathfrak{p}}$ with a canonical generator $s_{\mathfrak{p}}$ (the Frobenius).

Of course, if s_1 and s_2 are two distinct generators of H, the sets of corresponding primes p are disjoint (e.g., take the cyclotomic field $K = \mathbb{Q}(\zeta_5)$ of fifth roots of unity and $H = G$ (cyclic of order $h = 4$), with $\zeta_5^{s_1} = \zeta_5^2$ and $\zeta_5^{s_2} = \zeta_5^3$; this characterizes the sets $\{p : \ p \equiv 2 \pmod 5\}$ and $\{p : \ p \equiv 3 \pmod 5\}$, respectively); see, e.g., [5, Section 3 of Chapter 7], [8, Section 3 of Appendix], or [1, Sections 1.1, 1.2, 4.6, of Chapter II] for Chebotarev's density theorem and properties of Frobenius automorphisms.

But we consider such a fixed residue degree $h \mid n$ since we shall see that the statement of our main result, on the order of $\eta \in K^\times$ modulo a prime ideal $\mathfrak{p}$, does not depend on the conjugate of the decomposition group $H_{\mathfrak{p}}$ of $\mathfrak{p}$, nor on its Frobenius $s_{\mathfrak{p}}$, but only on the residue degree n_p of the corresponding prime number p under $\mathfrak{p}$ (in other words, we shall classify the set of unramified prime ideals $\mathfrak{p}$ of K by means of the sole criterion $n_p = h$; so, any of the $\mathfrak{p}$, with $n_p = h$, would have the common property, depending on h, given by our main theorem).

Since the $h \mid n$ are finite in number, everything is effective (e.g., $h \in \{1, 2, 3\}$ for a dihedral group $G = D_6$, but $h \in \{1, 2\}$ for the Galois group of any compositum of quadratic fields).

1.2. Orders modulo $\mathfrak{p}$ and modulo p. Let $\eta \in K^\times$. In the sequel we shall assume that the multiplicative $\mathbb{Z}[G]$-module $\langle \eta \rangle_G$ generated by η is of $\mathbb{Z}$-rank n (i.e., $\langle \eta \rangle_G \otimes \mathbb{Q} \simeq \mathbb{Q}[G]$), but this is not needed for the following definition.

Definition 1.1. *Let p be a prime number, unramified in $K/\mathbb{Q}$, prime to η, and let $\mathfrak{p}$ be a prime ideal of K dividing p.*

We define the order of η modulo $\mathfrak{p}$ *(denoted $o_{\mathfrak{p}}(\eta)$) to be the least nonzero integer k such that $\eta^k \equiv 1 \pmod{\mathfrak{p}}$.*

We define the order of η modulo p *(denoted $o_p(\eta)$) to be the least nonzero integer k such that $\eta^k \equiv 1 \pmod{p}$.*

Of course, $o_{\mathfrak{p}}(\eta)$ and $o_p(\eta) = \mathrm{lcm}(o_{\mathfrak{p}}(\eta),\ \mathfrak{p} \mid p)$ divide $p^{n_p} - 1$, where n_p is the residue degree of p in $K/\mathbb{Q}$, but we intend to prove (see Theorem 2.1 for a more complete and general statement):

Let $h \mid n$ be a possible residue degree in $K/\mathbb{Q}$. Let $\eta \in K^\times$ be such that the multiplicative $\mathbb{Z}[G]$-module generated by η is of $\mathbb{Z}$-rank n. Then for all large enough prime p (denoted $p \gg 0$ in all the paper) with residue degree $n_p = h$, the orders $o_{\mathfrak{p}}(\eta)$ for any $\mathfrak{p} \mid p$, and $o_p(\eta)$ do not divide any of the integers

$$D_{h,\delta}(p) := \frac{p^h - 1}{\Phi_\delta(p)}, \quad \delta \mid h$$

where $\Phi_\delta(X)$ is the δth cyclotomic polynomial.

Consider, for any unramified prime p, the characteristic property of the Frobenius automorphism $s_{\mathfrak{p}}$ of $\mathfrak{p} \mid p$ in $K/\mathbb{Q}$,

$$\eta^{s_{\mathfrak{p}}} \equiv \eta^p \pmod{\mathfrak{p}}.$$

Let $H_{\mathfrak{p}} := \langle s_{\mathfrak{p}} \rangle$ be the decomposition group of $\mathfrak{p}$ (denoted H to simplify) and let $\sigma \in G/H$ (or a representative in G); the Frobenius $s_{\mathfrak{p}^\sigma}$ of $\mathfrak{p}^\sigma$ is $s_{\mathfrak{p}}^\sigma := \sigma \cdot s_{\mathfrak{p}} \cdot \sigma^{-1}$ and we get $\eta^{s_{\mathfrak{p}^\sigma}} \equiv \eta^p \pmod{\mathfrak{p}^\sigma}$. So, if $s_{\mathfrak{p}}$ and σ commute this leads to $s_{\mathfrak{p}}^\sigma = s_{\mathfrak{p}^\sigma} = s_{\mathfrak{p}}$ and $\eta^{s_{\mathfrak{p}}} \equiv \eta^p \pmod{\mathfrak{p}^\sigma}$. In other words, we have

$$\eta^{s_{\mathfrak{p}}} \equiv \eta^p \quad \Big(\mathrm{mod} \prod_{\substack{\sigma \in G/H \\ \sigma . s_{\mathfrak{p}} = s_{\mathfrak{p}} . \sigma}} \mathfrak{p}^\sigma\Big).$$

In the Abelian case, we get (independently of the choice of $\mathfrak{p} \mid p$)

$$\eta^{s_{\mathfrak{p}}} \equiv \eta^p \pmod{p}.$$

Lemma 1.2. *Let $\eta \in K^\times$ be such that the multiplicative $\mathbb{Z}[G]$-module $\langle \eta \rangle_G$ is of $\mathbb{Z}$-rank n and let $\mu(K)$ be the group of roots of unity of K. Let H be a cyclic subgroup of G and let s be any generator of H; let $f(X) \in \mathbb{Z}[X]$ be a given polynomial such that $f(s) \neq 0$ in $\mathbb{Z}[H]$.*

Then, for all prime numbers $p \gg 0$ such that there exists a prime ideal $\mathfrak{p} \mid p$ for which $s_{\mathfrak{p}} = s$, whenever $\zeta \in \mu(K)$ we have

$$\eta^{f(p)} \not\equiv \zeta \pmod{\mathfrak{p}}.$$

Proof. We have $\eta^{f(p)} \equiv \eta^{f(s)} \pmod{\mathfrak{p}}$; thus, if $\eta^{f(p)} \equiv \zeta \pmod{\mathfrak{p}}$ for some ζ, this leads to $\eta^{f(s)} - \zeta \equiv 0 \pmod{\mathfrak{p}}$ giving, by the norm in $K/\mathbb{Q}$,

$$\mathrm{N}_{K/\mathbb{Q}}(\eta^{f(s)} - \zeta) \equiv 0 \pmod{p^{|H|}}.$$

Since $\langle \eta \rangle_G$ is of multiplicative $\mathbb{Z}$-rank n and $f(s) \neq 0$, we have $\eta^{f(s)} \notin \mu(K)$; then $\mathrm{N}_{K/\mathbb{Q}}(\eta^{f(s)} - \zeta)$ is a nonzero rational constant depending only on η, $f(s)$, ζ, and whose numerator is in $p^{|H|}\mathbb{Z}$ (a contradiction for $p \gg 0$). $\square$

The statement of the lemma does not depend on the choice of s generating H, nor on the choice of the prime ideal $\mathfrak{p} \mid p$ such that $s_{\mathfrak{p}} = s$ (in the Abelian case, any $\mathfrak{p} \mid p$ is suitable since $s_{\mathfrak{p}^\sigma} = s_{\mathfrak{p}}$ for all $\sigma \in G$).

If $s \in G$ is of order $h \geq 1$, any nonzero element of $\mathbb{Z}[H]$ can be writen $f(s)$ where $f(X)$ is of degree $< h$; if we take $f(X)$ of degree 0, then we have $f(s) = f \in \mathbb{Z} \setminus \{0\}$ regardless of h and s, giving the obvious result

$$\eta^f \not\equiv \zeta \pmod{\mathfrak{p}} \quad \text{for any } p \gg 0 .$$

Naturally, an interesting application of this Lemma is when $f(X) \mid X^h - 1$ in $\mathbb{Z}[X]$, $f(X) \neq X^h - 1$, and when the degree of $f(X)$ is maximal. This explains why the case $h = n_p = 1$ (p totally split in $K/\mathbb{Q}$) is uninteresting since $f(X) \mid X - 1$, with $f(X) \neq X - 1$, gives $f = 1$ and the same conclusion as above.

2. Consequences for the values of $o_{\mathfrak{p}}(\eta)$ and $o_p(\eta)$

We have the factorization

$$p^h - 1 = \prod_{\delta \mid h} \Phi_\delta(p) ,$$

where $\Phi_\delta(X)$ is the δth cyclotomic polynomial (see [8, Chapter 2]). So we can consider the divisors $\prod_{\delta \in I} \Phi_\delta(p)$, where I is any strict subset of the set of divisors of h. Of course, it will be sufficient to restrict ourselves to *maximal* subsets I, which gives the divisors $D_{h,\delta}(p) := \frac{p^h - 1}{\Phi_\delta(p)}$, $\delta \mid h$. For instance, if $h = 6$, we get the set

$$\{p^5+p^4+p^3+p^2+p+1,\ p^5-p^4+p^3-p^2+p-1,\ p^4-p^3+p-1,\ p^4+p^3-p-1\},$$

giving the complete set of "polynomial divisors" of $p^6 - 1$,

$$\begin{aligned} \{&1, p-1, p+1, p^2-1, p^2-p+1, p^3-2\,p^2+2\,p-1, p^3+1, \\ &p^4-p^3+p-1, p^2+p+1, p^3-1, p^3+2\,p^2+2\,p+1, p^4+p^3-p-1, \\ &\quad p^4+p^2+1, p^5-p^4+p^3-p^2+p-1, p^5+p^4+p^3+p^2+p+1\} . \end{aligned}$$

Theorem 2.1. *Let $K/\mathbb{Q}$ be Galois of degree n, of Galois group G. Let $h \mid n$ be a possible residue degree in $K/\mathbb{Q}$. Let $\mu(K)$ be the group of roots of unity contained in K. Let $\eta \in K^\times$ be such that the multiplicative $\mathbb{Z}[G]$-module generated by η is of $\mathbb{Z}$-rank n.*

Then for all (unramified) prime number $p \gg 0$, with residue degree $n_p = h$, and for any prime ideal $\mathfrak{p} \mid p$, the least integer $k \geq 1$ for which there exists $\zeta \in \mu(K)$ such that $\eta^k \equiv \zeta \pmod{\mathfrak{p}}$ is a divisor of $p^h - 1$ which does not divide any of the integers

$$D_{h,\delta}(p) := \frac{p^h - 1}{\Phi_\delta(p)} , \quad \delta \mid h ,$$

where $\Phi_\delta(X)$ is the δth cyclotomic polynomial.

Hence $o_{\mathfrak{p}}(\eta)$ and a fortiori $o_p(\eta)$ (cf. Definition 1.1), do not divide any of the $D_{h,\delta}(p)$.

Proof. Let $k' = \gcd(k, p^h - 1)$. Then we have $k' = \lambda\, k + \mu\, (p^h - 1)$, $\lambda, \mu \in \mathbb{Z}$, and $\eta^{k'} \equiv \eta^{\lambda\, k} \equiv \zeta^{\lambda} =: \zeta' \pmod{\mathfrak{p}}$; but $k' \mid k$, so $k = k' \mid p^h - 1$. Suppose that k divides some $D_{h,\delta}(p) = \frac{p^h-1}{\Phi_\delta(p)} = \prod_{\delta' \mid h,\, \delta' \neq \delta} \Phi_{\delta'}(p)$. Let s be the Frobenius of $\mathfrak{p}$ and $H = \langle s \rangle$ its decomposition group (of order h). Thus $\eta^k \equiv \zeta \pmod{\mathfrak{p}}$ yields

$$\eta^{D_{h,\delta}(p)} \equiv \zeta' \pmod{\mathfrak{p}}, \quad \zeta' \in \mu(K),$$

giving

$$\eta^{D_{h,\delta}(p)} \equiv \eta^{D_{h,\delta}(s)} \equiv \zeta' \pmod{\mathfrak{p}}.$$

From $\mathbb{Z}[H] \simeq \mathbb{Z}[X]/(X^h - 1)\,\mathbb{Z}[X]$, we get in $\mathbb{Z}[H]$

$$D_{h,\delta}(s) = \prod_{\delta' \mid h,\, \delta' \neq \delta} \Phi_{\delta'}(s) \neq 0$$

since $D_{h,\delta}(X) \notin (X^h - 1)\,\mathbb{Z}[X]$; the polynomial $D_{h,\delta}(X) \in \mathbb{Z}[X]$ being independent of p, Lemma 1.2 applied to $f(X) = D_{h,\delta}(X)$ gives a contradiction for all $p \gg 0$ with residue degree $n_p = h$. □

If $\langle \eta \rangle_G$ is not of $\mathbb{Z}$-rank n, a statement does exist which depends on the G-representation $\langle \eta \rangle_G$; for instance, let $K = \mathbb{Q}(\sqrt{m})$ and $\eta \in K^\times \setminus \mu(K)$:

- If $\mathrm{N}_{K/\mathbb{Q}}(\eta) = \pm 1$, then $o_p(\eta) \nmid D_{2,2}(p) = p - 1$ for all prime $p \gg 0$, inert in $K/\mathbb{Q}$.
- If $\eta^{1-s} = \pm 1$, then $o_p(\eta) \nmid D_{2,1}(p) = p + 1$ (e.g., $\eta = \sqrt{m}$, $m \neq -1$).

The expression *"for all $p \gg 0$ of residue degree $n_p = h$"* in the theorem is effective and depends, numerically, only on h and the conjugates of η.

The theorem gives the generalization of the particular case $h = 2$ in [2].

In the above case $h = 6$ and $p \gg 0$ (with $n_p = 6$), the orders $o_{\mathfrak{p}}(\eta)$ are divisors of $p^6 - 1$ which are not divisors of any of the integers in the set:

$$\{\, p^5+p^4+p^3+p^2+p+1,\ p^5-p^4+p^3-p^2+p-1,\ p^4-p^3+p-1,\ p^4+p^3-p-1\}.$$

For $p = 7$ and $h = 6$, we have 60 divisors of $p^6 - 1 = 2^4 \cdot 3^2 \cdot 19 \cdot 43$, and the distinct divisors of these 4 polynomials are the 52 integers:

$$1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 19, 24, 36, 38, 43, 48, 57, 72, 76, 86, 114, 129, 144,$$
$$152, 171, 172, 228, 258, 304, 342, 344, 387, 456, 516, 684, 688, 774, 817, 912,$$
$$1032, 1368, 1634, 2064, 2451, 2736, 3268, 4902, 6536, 7353, 9804, 14706, 19608.$$

So the remaining (possible) divisors of $p^6 - 1$ are

$$1548, 3096, 6192, 13072, 29412, 39216, 58824, 117648.$$

Of course, in our example, the prime $p = 7$ is too small regading η, but the interesting fact (which is similar for larger p and any integer h) is the great number of impossible divisors of $p^h - 1$ for small numbers η.

For $p = 1093$ (resp. 504202701918008951235073), only 76 (resp. 242424) divisors are possible among the 384 (resp. 518144) divisors of $p^6 - 1$.

The case $h = \ell$ (a prime) implies that $o_{\mathfrak{p}}(\eta)$ is not a divisor of $p-1$ nor a divisor of $p^{\ell-1}+\cdots+p+1$ for $p \gg 0$ with residue degree $n_p = \ell$; this means that $o_{\mathfrak{p}}(\eta) = d_1 d_2$ with $d_1 \mid p-1$, $d_1 \neq 1$, $d_2 \mid p^{\ell-1} + \cdots + p + 1$, $d_2 \neq 1$ (taking care of the fact that when $p \equiv 1 \pmod{\ell}$, we have the relation $\gcd(p-1, p^{\ell-1} + \cdots + p + 1) = \ell$).

Remark 2.2. It is clear that if $r \in \mathbb{N} \setminus \{0\}$ is small, Theorem 2.1 implies that for all prime $p \gg 0$ with residue degree $n_p = h$ and for any $\mathfrak{p} \mid p$, the least integer $k \geq 1$ for which there exists $\zeta \in \mu(K)$ such that $\eta^k \equiv \zeta \pmod{\mathfrak{p}}$ cannot divide any of the integers $r \cdot D_{h,\delta}(p)$, $\delta \mid h$ (indeed, η^r is still small in an Archimedean point of view). This makes sense only when $r = r_\delta$ is choosen, for each $D_{h,\delta}(p)$, as a small divisor of $\Phi_\delta(p)$.

So the probability of $o_{\mathfrak{p}}(\eta) \mid r_\delta \cdot D_{h,\delta}(p)$ increases (from 0 to 1) when the factor $r_\delta \mid \Phi_\delta(p)$ increases (from $r_\delta = 1$ to $r_\delta = \Phi_\delta(p)$). In the example $h = \ell$, where $o_{\mathfrak{p}}(\eta) = d_1 d_2$, $d_1 \mid p-1$, $d_2 \mid p^{\ell-1} + \cdots + p + 1$, we have d_1 and $d_2 \to \infty$ for $p \to \infty$.

3. A numerical example

Let $K = \mathbb{Q}(x)$ be the cyclic cubic field of conductor 7 defined by $x = \zeta_7 + \zeta_7^{-1}$ from a primitive seventh root of unity ζ_7; its irreducible polynomial is $X^3 + X^2 - 2X - 1$.

Let $\eta = 8\,x + 5$ of norm -203; then for $p < 200$, inert in K (i.e., $p^2 \not\equiv 1 \pmod{7}$), we obtain the exceptional example $o_{17}(\eta) = 307 = p^2 + p + 1$ and no other when p increases; we get some illustrations with a small $r \mid p-1$, $r > 1$ (e.g., $p = 101$, $r = 2$, with $o_p(\eta) = r \cdot (p^2 + p + 1)$), according to the following numerical results; note that when $p \equiv 1 \pmod{3}$, we have $o_p(\eta) = \frac{1}{3} \cdot \gcd(o_p(\eta), p-1) \cdot \gcd(o_p(\eta), p^2 + p + 1)$:

(1) $p \equiv 2 \pmod{7}$:

p	$\gcd(o_p(\eta), p-1)$	$\gcd(o_p(\eta), p^2+p+1)$
2	1	1
23	11	553
37	36	201
79	78	6321
107	53	11557
149	37	22351
163	54	26733
191	190	36673

(2) $p \equiv 3 \pmod 7$:

p	$\gcd(o_p(\eta), p-1)$	$\gcd(o_p(\eta), p^2+p+1)$
3	1	13
17^*	1	307
31	15	993
59	58	3541
73	9	5403
101^{**}	2	10303
157	26	8269
199	198	39801

(3) $p \equiv 4 \pmod 7$:

p	$\gcd(o_p(\eta), p-1)$	$\gcd(o_p(\eta), p^2+p+1)$
11	10	133
53	26	2863
67	33	4557
109	27	11991
137	136	18907
151	75	22953
179	89	32221
193	192	37443

(4) $p \equiv 5 \pmod 7$:

p	$\gcd(o_p(\eta), p-1)$	$\gcd(o_p(\eta), p^2+p+1)$
5	4	31
19	9	381
47	23	2257
61	10	1261
89	11	8011
103	102	10713
131	65	17293
173	172	30103

With the same data, the least values of $\gcd(o_p(\eta), p-1)$ are:

- 1 (for $p = 2$, 3, 17), 2 (for $p = 101$), 3 (for $p = 13669$, for wich we get $o_p(\eta) = 560565693$), 4 (for $p = 5$, 317), 9 (for $p = 19$, 73).
- Up to $p \leq 10^7$, we have no other solutions for $\gcd(o_p(\eta), p-1) < 10$.
- For $\gcd(o_p(\eta), p^2+p+1) < 100$ we get 1 (for $p = 2$), 13 (for $p = 3$), 31 (for $p = 5$); for $\gcd(o_p(\eta), p^2+p+1) < 1000$ we only have the primes $p = 2, 3, 5, 11, 17, 19, 23, 31, 37$ giving a solution up to 10^7.

4. A lower bound for $o_p(\eta)$

When η is fixed in $K^\times$, very small orders are impossible as $p \to \infty$ because of the following theorem giving Archimedean constraints; in this result none hypothesis is done on the rank of the multiplicative $\mathbb{Z}[G]$-module generated by η (except that this $\mathbb{Z}$-rank is assumed to be $\neq 0$) nor on the field K itself. We denote by Z_K the ring of integers of K.

Theorem 4.1. *Let $\mu(K)$ be the group of roots of unity contained in K. Let $\eta \in K^\times \setminus \mu(K)$ and $\nu \in \mathbb{N} \setminus \{0\}$ be such that $\nu\,\eta \in Z_K$. Then, for any p prime to η and ν, the congruence $\eta^k \equiv \zeta \pmod{p}$, $\zeta \in \mu(K)$, $k \geq 1$, implies the inequality*

$$k \geq \frac{\log(p) - \log(2)}{\max\big(\log(\nu \cdot c_0(\eta)), \log(\nu)\big)},$$

where $c_0(\eta) = \max_{\sigma \in G}(|\eta^\sigma|)$. If $\eta \in Z_K$ (i.e., $\nu = 1$), then we get $k \geq \frac{\log(p-1)}{\log(c_0(\eta))}$. In other words, if $Z_{K,(p)}$ is the ring of p-integers of K, the order of the image of η in $Z_{K,(p)}/\mu(K)\cdot(1+p\,Z_{K,(p)})$, and a fortiori $o_p(\eta)$, satisfies the above inequalities.

Proof. Put $\eta = \frac{\theta}{\nu}$, with $\theta \in Z_K$. The congruence is equivalent to $\theta^k = \zeta\,\nu^k + \Lambda\,p$, where $\Lambda \in Z_K \setminus \{0\}$ (because $\eta \notin \mu(K)$). Taking a suitable conjugate of this equality, we can suppose $|\Lambda| \geq 1$. Thus

$$|\Lambda|\,p = |\theta^k - \zeta\,\nu^k| \leq |\theta|^k + \nu^k$$

giving $|\theta|^k + \nu^k \geq p$; so, using a conjugate θ_0 such that $|\theta_0| = \max_{\sigma \in G}(|\theta^\sigma|)$, we have a fortiori $|\theta_0|^k + \nu^k \geq p$, with $|\theta_0| \geq 1$ since $\theta \in Z_K$.

(1) If $\nu \geq 2$, then

$$p \leq |\theta_0|^k + \nu^k \leq 2\,\max(|\theta_0|^k, \nu^k)$$

giving the result.

(2) The case $\nu = 1$, used in [2, Lemme 6.2], gives $|\theta_0|^k \geq p - 1$, hence the upper bound $k \geq \frac{\log(p-1)}{\log(c_0(\eta))}$ since $|\theta_0| = c_0(\eta) > 1$ (because $\eta \notin \mu(K)$). □

Under the assumptions of Theorem 2.1 we have the following result.

Corollary 4.2. *Suppose to simplify that $\eta \in Z_K$; let p be unramified of residue degree n_p such that for some $\delta \mid n_p$, $o_p(\eta) = r \cdot d$, $d \mid D_{n_p,\delta}(p)$, $r = r_\delta \mid \Phi_\delta(p)$ (cf. Remark 2.2). Then $r \geq \frac{\log(p-1)}{\log(c_0(\eta^{D_{n_p,\delta}(s)}))}$, where s generates any decomposition group of p.*

In the previous example of Section 3, for $p \approx 10^7$ and $o_p(\eta) = r \cdot d$, $d \mid D_{3,\delta}(p)$, we find, from the corollary, $r \geq 3$ for $\delta = 1$ (i.e., $r \mid p-1$), $r \geq 9$ for $\delta = 3$ (i.e., $r \mid p^2 + p + 1$).

5. Densities–Probabilities for $o_{\mathfrak{p}}(\eta)$ and $o_p(\eta)$

In this section, we examine some probabilistic aspects concerning the orders modulo $\mathfrak{p} \mid p$ of an $\eta \in K^\times$. For any p, unramified in $K/\mathbb{Q}$, recall that g_p is the number of prime ideals $\mathfrak{p} \mid p$ and n_p the common residue degree of these ideals. Let Z_K be the ring of integers of K; the residue fields $F_{\mathfrak{p}} = Z_K/\mathfrak{p}$ are isomorphic to $\mathbb{F}_{p^{n_p}}$.

5.1. Densities. It is assumed in this short subsection that p is fixed and that $\eta \in K^\times$ is a variable modulo p, prime to the given p; in other words, η varies in the group $(Z_{K,(p)}/p\,Z_{K,(p)})^\times$ of invertible elements of the quotient $Z_{K,(p)}/p\,Z_{K,(p)}$, where $Z_{K,(p)}$ is the ring of p-integers of K, so that we have

$$(Z_{K,(p)}/p\,Z_{K,(p)})^\times \simeq \prod_{\mathfrak{p}\mid p} F_{\mathfrak{p}}^\times \quad (p \text{ unramified}).$$

For each prime ideal $\mathfrak{p} \mid p$, let $\eta_{\mathfrak{p}} \in F_{\mathfrak{p}}^\times$ be the residue image of η at $\mathfrak{p}$.

The density of numbers η, whose diagonal image is given in $\prod_{\mathfrak{p}\mid p} F_{\mathfrak{p}}^\times$, is

$$\frac{1}{(p^{n_p}-1)^{g_p}}$$

because the map $\eta \pmod{p} \mapsto (\eta_{\mathfrak{p}})_{\mathfrak{p}\mid p} \in \prod_{\mathfrak{p}\mid p} F_{\mathfrak{p}}^\times$ yields an isomorphism (from chinese remainder theorem) and, in some sense, the g_p conditions on the $\eta_{\mathfrak{p}}$, $\mathfrak{p} \mid p$, are independent as η varies (the notion of density is purely algebraic and the previous Archimedean obstructions of Sections 2 and 4 do not exist). Thus the orders $o_{\mathfrak{p}}(\eta)$ and $o_p(\eta)$ have canonical densities (see §5.4).

5.2. Probabilities and Independence. We shall speak of probabilities when, on the contrary, $\eta \in K^\times \setminus \mu(K)$ is fixed and when $p \to \infty$ is the variable; but to avoid trivial cases giving obvious obstructions (as $\eta \in \mathbb{Q}^\times$ for which $o_p(\eta) \mid p-1$ for any p regardless of the residue degree of p; see §5.3 for more examples), we must put some assumptions on η so that $o_p(\eta)$ can have any *possible value* dividing $p^{n_p}-1$ (by reference to Theorem 2.1, Remark 2.2, and Theorem 4.1 giving moreover theoretical limitations for the orders, so that the true probabilities are significantly lower).

Let H be the decomposition group of a prime ideal $\mathfrak{p}_0 \mid p$, p unramified in $K/\mathbb{Q}$. Considering $F_{\mathfrak{p}_0}^\times$ as a H-module (H is generated by the global Frobenius $s = s_{\mathfrak{p}_0}$ which by definition makes sense in $F_{\mathfrak{p}_0}/\mathbb{F}_p$), $\prod_{\mathfrak{p}\mid p} F_{\mathfrak{p}}^\times$ is the induced representation and we get $\prod_{\mathfrak{p}\mid p} F_{\mathfrak{p}}^\times = \bigoplus_{\sigma\in G/H} \sigma F_{\mathfrak{p}_0}^\times$ where $\sigma F_{\mathfrak{p}_0}^\times = F_{\mathfrak{p}_0^\sigma}^\times$ for all $\sigma \in G/H$ (using additive notation for convenience).

In the same way, the representation $\langle\eta\rangle_G$ can be written $\langle\eta\rangle_G = \sum_{\sigma\in G/H} \sigma\langle\eta\rangle_H$, where $\langle\eta\rangle_H$ is the multiplicative $\mathbb{Z}[H]$-module generated by η. So, for natural congruential reasons (that must be valid regardless of the prime p) concerning the map $\eta \pmod p \mapsto (\eta_{\mathfrak{p}})_{\mathfrak{p}|p}$, the representation $\langle\eta\rangle_G$ must be induced by the H-representation $\langle\eta\rangle_H$, i.e., we must have

$$\langle\eta\rangle_G = \bigoplus_{\sigma\in G/H} \sigma\langle\eta\rangle_H$$

(otherwise, any nontrivial $\mathbb{Z}$-relation between the conjugates of η will give non-independent variables $\eta_{\mathfrak{p}}$ in a probabilistic point of view). Since any cyclic subgroup H of G is realizable as a decomposition group when p varies, the above must work for any H; taking $H = 1$, we obtain that $\langle\eta\rangle_G = \bigoplus_{\sigma\in G}\langle\eta^\sigma\rangle_{\mathbb{Z}}$ which is equivalent for $\langle\eta\rangle_G$ to be of $\mathbb{Z}$-rank n, giving the following heuristic in relation with the properties of the normalized p-adic regulator of η studied in [2].

Heuristic 5.1. *Let $K/\mathbb{Q}$ be Galois of degree n, of Galois group G. Consider $\eta \in K^\times$ and, for any prime number $p \gg 0$, unramified in $K/\mathbb{Q}$ and prime to η, let $(\eta_{\mathfrak{p}})_{\mathfrak{p}|p}$ be the diagonal image of η in $\prod_{\mathfrak{p}|p} F_{\mathfrak{p}}^\times$.*

The components $\eta_{\mathfrak{p}}$ are independent*, in the meaning that for given $a_{\mathfrak{p}} \in F_{\mathfrak{p}}^\times$,*

$$\mathrm{Prob}\,(\eta_{\mathfrak{p}} = a_{\mathfrak{p}},\ \forall\,\mathfrak{p} \mid p) = \prod_{\mathfrak{p}|p} \mathrm{Prob}\,(\eta_{\mathfrak{p}} = a_{\mathfrak{p}}),$$

if and only if η generates a multiplicative $\mathbb{Z}[G]$-module of $\mathbb{Z}$-rank n.

5.3. Remarks and examples. Suppose that η generates a multiplicative $\mathbb{Z}[G]$-module of $\mathbb{Z}$-rank n, which has obvious consequences (apart the fact that $\eta \notin \mu(K)$):

(1) This implies that η is not in a strict subfield L of K; otherwise, if H is a non-trivial cyclic subgroup of G (hence of order $h > 1$) such that $L \subseteq K^H$, for any unramified prime p such that H is the decomposition group of $\mathfrak{p} \mid p$ with Frobenius s, $o_{\mathfrak{p}}(\eta)$ is not a random divisor of $p^h - 1$ but a divisor of $p - 1$, the residue field of K^H at $\mathfrak{p}$ being $\mathbb{F}_p$ for infinitely many p.

(2) In the same way, η cannot be an element of $K^\times$ of relative norm 1 in K/K^H, $H \neq 1$, because of the relation $\mathrm{N}_{K/K^H}(\eta) = 1$ giving

$$\eta^{p^{h-1}+\cdots+p+1} \equiv 1 \pmod{\mathfrak{p}}.$$

For the unit $\eta = 2\sqrt{2} + 3$ and any p inert in $\mathbb{Q}(\sqrt{2})$, we obtain $\eta^{p+1} \equiv 1 \pmod p$ (i.e., $o_p(\eta) \mid p + 1$), giving infinitely many p such that $o_p(\eta) < p$:

$$\begin{aligned}(p, o_p(\eta)) = {} & (29, 10), (59, 20), (179, 36), (197, 18), (227, 76),\\ & (229, 46), (251, 84), (269, 30), (293, 98), (379, 76),\\ & (389, 78), (419, 140), (443, 148), \ldots\end{aligned}$$

(3) Let $K = \mathbb{Q}(j, \sqrt[3]{2})$, where j is a primitive third root of unity, and let $\eta = \sqrt[3]{2} - 1$ (a unit of $\mathbb{Q}(\sqrt[3]{2})$); for the same reason with $H = \mathrm{Gal}(K/\mathbb{Q}(j))$, from $\eta^{s^2+s+1} = 1$, we get, for any prime p inert in $K/\mathbb{Q}(j)$,

$$\eta^{p^2+p+1} \equiv 1 \pmod{p}$$

(for $p = 7$, η is of order 19 modulo p and we have infinitely many p such that $o_p(\eta) \mid p^2 + p + 1$).

In such a non-Abelian case, some relations of dependence can also occur in a specific component $F_{\mathfrak{p}}^{\times}$, $\mathfrak{p} \mid p$. Since $\eta = \sqrt[3]{2} - 1 \in \mathbb{Q}(\sqrt[3]{2})$, for any $\mathfrak{p}$ inert in $K/\mathbb{Q}(\sqrt[3]{2})$ (i.e., $K^H = \mathbb{Q}(\sqrt[3]{2})$, in which case, p splits in $K/\mathbb{Q}(j)$), there exists a rational a such that $\sqrt[3]{2} \equiv a \pmod{\mathfrak{p}}$, $\sqrt[3]{2} \equiv a\, j^2 \pmod{\mathfrak{p}^s}$, $\sqrt[3]{2} \equiv a\, j \pmod{\mathfrak{p}^{s^2}}$. So $\eta \equiv a - 1 \pmod{\mathfrak{p}}$ and $o_{\mathfrak{p}}(\eta) \mid p - 1$ which is not necessary true for $o_p(\eta)$: for $p = 5$ we have $\sqrt[3]{2} \equiv 3 \pmod{\mathfrak{p}}$, $\sqrt[3]{2} \equiv 3j^2 \pmod{\mathfrak{p}^s}$, $\sqrt[3]{2} \equiv 3j \pmod{\mathfrak{p}^{s^2}}$. Then $\eta \equiv 2 \pmod{\mathfrak{p}}$ is of order 4 modulo $\mathfrak{p}$, but $\eta \equiv 3j^2 - 1 \pmod{\mathfrak{p}^s}$ is of order 8 modulo $\mathfrak{p}^s$. So $o_p(\eta) = 8$ but we have some constraints on the $\eta_{\mathfrak{p}}$.

5.4. Probabilities for the order of η modulo p. Now we suppose that the multiplicative $\mathbb{Z}[G]$-module $\langle \eta \rangle_G$ is of $\mathbb{Z}$-rank n.

Remark 5.2. From Theorem 2.1, we know that $o_p(\eta) \nmid D_{n_p,\delta}(p)$ for all $\delta \mid n_p$, when $p \to \infty$; in particular, $o_p(\eta) \nmid p - 1$ if we assume $n_p > 1$. For this, the hypothesis on the $\mathbb{Z}$-rank of $\langle \eta \rangle_G$ is fundamental. In other words, the probability of some (unbounded) orders is zero. This is strengthened by Remark 2.2. Moreover, Theorem 4.1 gives obstructions for very small orders, which decreases the probabilities of small orders; the total defect of probabilities is less than $O(\log(p))$ and is to be distributed among all orders, which is negligible. Thus, this favors large orders which are more probable; this goes in the good direction because we shall study probabilities of orders $o_p(\eta)$ less than p when $n_p > 1$.

Although the theoretical values of the probabilities are rather intricate, in a first approach, we can neglect these aspects and give some results in an heuristic point of view corresponding to the case where η is considered as a variable (so that probabilities coincide with known densities) and we use the heuristic that when η is fixed once for all, probabilities are much lower than densities as $p \to \infty$ as explained in §5.2. Furthermore, we shall use rough majorations (except in the quadratic case and $n_p = 2$, where densities are exact).

If $D \mid p^{n_p}-1$, $o_p(\eta) \mid D$ is equivalent to $\eta_{\mathfrak{p}}^D = 1$ for all $\mathfrak{p} \mid p$. So we obtain

$$\begin{aligned}\mathrm{Prob}\,\big(o_p(\eta) = D\big) &\le \mathrm{Prob}\,\big(o_p(\eta)\,|\,D\big)\\ &= \prod_{\mathfrak{p}\mid p} \mathrm{Prob}\,\big(\eta_{\mathfrak{p}}^D = 1\big) \quad \text{(cf. Heuristic 5.1)}.\end{aligned}$$

Since $F_{\mathfrak{p}}^{\times}$ is cyclic of order $p^{n_p}-1$, we get

$$\mathrm{Prob}\,\big(\eta_{\mathfrak{p}}^D = 1\big) = \sum_{d\mid D} \frac{\phi(d)}{p^{n_p}-1} = \frac{D}{p^{n_p}-1},$$

where ϕ is the Euler function, and we obtain, for any $D \mid p^{n_p}-1$,

$$\mathrm{Prob}\,\big(o_p(\eta) = D\big) \le \Big(\frac{D}{p^{n_p}-1}\Big)^{g_p}.$$

If $g_p = 1$, then $n_p = n$, and we can replace this inequality by

$$\mathrm{Prob}\,\big(o_p(\eta) = D\big) \le \mathrm{Density}\,\big(o_p(\eta) = D\big) = \frac{\phi(D)}{p^n - 1}.$$

When $g_p > 1$, the exact expression is more complicate since $o_p(\eta) = D$ if and only if $o_{\mathfrak{p}_0}(\eta_{\mathfrak{p}_0}) = D$ for at least one $\mathfrak{p}_0 \mid p$ and $o_{\mathfrak{p}}(\eta_{\mathfrak{p}}) \mid D$ for all $\mathfrak{p} \mid p$, $\mathfrak{p} \ne \mathfrak{p}_0$, but we shall not need it.

6. Probabilities of orders $o_p(\eta) < p$

Suppose $p \gg 0$, non totally split in $K/\mathbb{Q}$. In [2], the number η is a fixed *integer* of $K^{\times}$ and we have to consider the set

$$I_p(\eta) := \{1, [\eta]_p, \ldots, [\eta^k]_p, , \ldots, [\eta^{p-1}]_p\},$$

where $[\,\cdot\,]_p$ denotes a suitable residue modulo $p\,Z_K$. We need that $I_p(\eta)$ be a set with p distinct elements, to obtain valuable statistical results on the "local regulators $\Delta_p^{\theta}(z)$", $z \in I_p(\eta)$, to strengthen some important heuristics; this condition is equivalent to $\eta^k \not\equiv 1 \pmod p$ for all $k = 1, \ldots, p-1$, hence to $o_p(\eta) > p$.

So we are mainely interested by the computation of $\mathrm{Prob}\,\big(o_p(\eta) < p\big)$ when $n_p > 1$ and we intend to give an upper bound for this probability. As we know from Theorem 2.1, taking the example of quadratic fields we have, for $\langle\eta\rangle_G$ of $\mathbb{Z}$-rank 2,

$$o_p(\eta) \nmid p-1 \ \text{ and } \ o_p(\eta) \nmid p+1, \ \text{for } p \to \infty;$$

but $o_p(\eta) < p$ remains possible for small divisors D of p^2-1 (e.g., $\eta = 5+\sqrt{-1}$ for which $p = 19$ is inert in $\mathbb{Q}(\sqrt{-1})$ and $o_{19}(\eta) = 3\cdot 5$ whereas $p-1 = 18$ and $p+1 = 20$).

Suppose that $K \ne \mathbb{Q}$ and that the residue degree of p is $n_p > 1$. Let

$$\mathcal{D}_p := \{D : \ D \mid p^{n_p}-1, D < p, \ D \nmid D_{n_p,\delta}(p)\ \forall\,\delta \mid n_p\}.$$

Then we consider that we have, for all $p \gg 0$ of residue degree n_p, the following heuristic inequality (from Theorems 2.1, 4.1 and §5.4):

$$\begin{aligned}\text{Prob}\,\big(o_p(\eta) < p\big) &\leq \text{Prob}\,\big(o_p(\eta) \in \mathcal{D}_p\big) \\ &\leq \sum_{D \in \mathcal{D}_p} \Big(\frac{D}{p^{n_p}-1}\Big)^{g_p} = \frac{1}{(p^{n_p}-1)^{g_p}} \sum_{D \in \mathcal{D}_p} D^{g_p}.\end{aligned} \tag{6.1}$$

A trivial upper bound for $\sum_{D\in\mathcal{D}_p} D^{g_p}$ is $\sum_{k=1}^{p-1} k^{g_p} = O(1)\, p^{g_p+1}$, giving

$$\text{Prob}\,\big(o_p(\eta) < p\big) \leq \frac{O(1)}{p^{g_p(n_p-1)-1}}$$

for which the application of the Borel–Cantelli heuristic supposes the inequality $g_p(n_p-1) \geq 3$, giving possible obstructions for quadratic or cubic fields with p inert, and quartic fields with $n_p = 2$. Of course, if $g_p(n_p-1)$ increases, the heuristic becomes trivial and we can replace $\text{Prob}\,\big(o_p(\eta) < p\big)$ by $\text{Prob}\,\big(o_p(\eta) < p^\kappa\big)$, for some $\kappa > 1$ (see Remark 6.2 (i)). But we can remove the obstructions concerning the cubic and quartic cases using an analytic argument suggested by G. Tenenbaum:

Theorem 6.1. *Let $K/\mathbb{Q}$ be Galois of degree $n \geq 2$, of Galois group G, and let $\eta \in K^\times$ be such that the multiplicative $\mathbb{Z}[G]$-module generated by η is of $\mathbb{Z}$-rank n. For any prime number p, let g_p be the number of prime ideals $\mathfrak{p} \mid p$ and let n_p be the residue degree of p in $K/\mathbb{Q}$.*

Then, under the above heuristic inequality (6.1)*, for all unramified $p \gg 0$ such that $n_p > 1$, we have (where* $\log_2 = \log \circ \log$*)*

$$\text{Prob}\,\big(o_p(\eta) < p\big) \leq \frac{1}{p^{g_p\,(n_p-1)-\varepsilon}}\,, \quad \textit{with } \varepsilon = O\left(\frac{1}{\log_2(p)}\right).$$

Proof. Let $S_p := \sum_{D\in\mathcal{D}_p} D^{g_p}$; under the two conditions $D \mid p^{n_p}-1$, $D < p$, we get $S_p < \sum_{D \mid p^{n_p}-1} \left(\frac{p}{D}\right)^{g_p} D^{g_p} = p^{g_p} \cdot \tau(p^{n_p}-1)$, where $\tau(m)$ denotes the number of divisors of the integer m. From [6, Theorem I.5.4], we have, for all $c > \log(2)$ and for all $m \gg 0$,

$$\tau(m) \leq m^{\frac{c}{\log_2(m)}}.$$

Taking $c = 1$ and $m = p^{n_p}-1 < p^{n_p}$, this leads to $S_p < p^{g_p + \frac{n_p}{\log_2(p^{n_p}-1)}}$ for all $p \gg 0$. Thus

$$\begin{aligned}\text{Prob}(o_p(\eta) < p) \leq \frac{S_p}{(p^{n_p}-1)^{g_p}} &\leq \frac{1}{(p^{n_p}-1)^{g_p} \cdot p^{-g_p - \frac{n_p}{\log_2(p^{n_p}-1)}}} \\ &= \frac{1}{p^{g_p\,(n_p-1) - O\left(\frac{1}{\log_2(p)}\right)}}.\end{aligned}$$

□

To apply the Borel–Cantelli heuristic giving the finiteness of primes p such that $o_p(\eta) < p$, we must have the inequality $g_p\,(n_p-1) \geq \varepsilon + 1$, hence $g_p\,(n_p-1) \geq 2$. Otherwise, we get $g_p = 1$ and $n_p = 2$, not sufficient to conclude for quadratic fields with p inert since, in this case,

$$\mathrm{Prob}(o_p(\eta) < p) \leq \frac{1}{p^{1-\varepsilon}} \quad \text{with } \varepsilon = O\left(\frac{1}{\log_2(p)}\right).$$

Remarks 6.2. (1) Still when $g_p\,(n_p-1) \geq 2$, we can replace the previous inequality $\mathrm{Prob}\,(o_p(\eta) < p) \leq \frac{1}{p^{g_p\,(n_p-1)-\varepsilon}}$ by

$$\mathrm{Prob}\,(o_p(\eta) < p^\kappa) \leq \frac{1}{p^{g_p\,(n_p-1)-\varepsilon}}$$

which is true for any real κ such that $1 \leq \kappa \leq n_p - \frac{1+\varepsilon}{g_p}$, in which case the Borel–Cantelli heuristic applies and may have some interest for large n_p; for instance, if $K = \mathbb{Q}_r$ is the subfield of degree ℓ^r (ℓ a prime, $r \geq 1$), of the cyclotomic $\mathbb{Z}_\ell$-extension of $\mathbb{Q}$, and if we take primes p totally inert in $K/\mathbb{Q}$, one can take $\kappa = \ell^r - 2$ (if $\ell^r \neq 2$) for any η as usual.

(2) Note that the proof of the theorem does not take into account the conditions $o_p(\eta) \nmid D_{n_p,\delta}(p)$ and it should be interesting to improve this aspect. But this theorem is a first step, and in the next sections, we intend to use explicitely the set $\mathcal{D}_p$ for numerical computations and for a detailed study of the more ambiguous quadratic fields case. Indeed, in this case, we have to estimate the more precise upper bound $\frac{1}{p^2-1}\sum_{D\in\mathcal{D}_p}\phi(D)$ and a numerical experiment with the following PARI program (from [7]) shows a great dispersion of the number N of such divisors:

```
{b=10^5; B=b+10^3; forprime(p=b, B, N=0; my(e=kronecker(-4,p));
F1=factor(2*(p-e)); F2=factor((p+e)/2); P=concat(F1[,1],F2[,1]);
E=concat(F1[,2],F2[,2]);
forvec(v=vectorv(# E,i,[0,E[i]]), my(d=factorback(P,v));
if(d>=p-1, next); if((p-1)%d!=0 && (p+1)%d!=0, N=N+1)); print(p," ", N))}
```

giving for instance (depending on the factorizations of $p-1$ and $p+1$):

- $p = 100237$, $N = 3$, where $(p-1)\cdot(p+1) = (2^2\cdot 3\cdot 8353)\cdot(2\cdot 50119)$,
- $p = 100673$, $N = 489$, where $(p-1)\cdot(p+1) = (2^6\cdot 11^2\cdot 13)\cdot(2\cdot 3^2\cdot 7\cdot 17\cdot 47)$.

We shall return more precisely to the quadratic case in §8.4.

We can state to conclude this section:

Conjecture 6.3. *Let $K/\mathbb{Q}$ be Galois of degree $n \geq 3$, of Galois group G. Let $\eta \in K^\times$ be such that the multiplicative $\mathbb{Z}[G]$-module generated by η is* *of $\mathbb{Z}$-rank n. For any unramified prime p, prime to η, let $o_p(\eta)$ be the order of η modulo p.*

Then $o_p(\eta) > p$, for all p non totally split in $K/\mathbb{Q}$, except a finite number. More generaly, $o_p(\eta) > p^{(n_p-1)+1-\frac{n_p}{n}\cdot(1+\varepsilon)}$, for all p such that $n_p > 1$, except a finite number.

7. Numerical evidences for the above conjecture

This section is independent of any $\eta \in K^\times$ and any number field K but depends only on *given and fixed* integer parameters denoted by abuse (n_p, g_p). For $n_p > 1$, we explicitely compute, for any p, $S_p := \sum_{D\in\mathcal{D}_p} D^{g_p}$ and the upper bound $\frac{S_p}{(p^{n_p}-1)^{g_p}}$ of $\mathrm{Prob}\,(o_p(\eta) < p)$, using the program described below. Recall that

$$\mathcal{D}_p := \{D :\ D \mid p^{n_p} - 1,\ D < p,\ D \nmid D_{n_p,\delta}(p)\ \forall\,\delta \mid n_p\}.$$

7.1. General program about the divisors $\boldsymbol{D \in \mathcal{D}_p}$. It is sufficient to precise the integers $n_p > 1$, $g_p \geq 1$, and the interval $[b, B]$ of primes p. The program gives the least value C_b^B of $C(p)$, $p \in [b, B]$, where

$$\frac{S_p}{(p^{n_p}-1)^{g_p}} =: \frac{1}{p^{C(p)}}\,.$$

The favourable cases for the Borel–Cantelli principle are those with $C_b^B > 1$, but the inequalities $C_b^B \geq C_b^\infty := \mathrm{Inf}_{p\in[b,\infty]}\,C(p)$ do not mean that the Borel–Cantelli principle applies since we ignore if $C_b^\infty > 1$ or not for $b \gg 0$, because C_b^∞ is an increasing function of b.

In the applications given below, n_p is a prime number, for which $D_{n_p,\delta}(p)$ is in $\{p-1,\, p^{n_p-1} + \cdots + p + 1\}$; for more general values of n_p, one must first compute the set $\mathcal{D}_p$ as defined in Theorem 2.1.

```
{b=10^6; B=10^7; gp=1; np=2; CC= gp*(np-1)+1; C=CC; V=vector(B,i,i^gp);
forprime(p=b, B, my(S=0, M=p^np-1, m=p-1, mm=M/m, i);
fordiv(M,d,if(d>p, break); if(m%d!=0 && mm%d!=0, S+=V[d]));
if(S!=0, C=(gp*log(M)-log(S))/log(p)); if(C<CC, CC=C)); print(CC)}
```

The initial $CC := g_p\,(n_p - 1) + 1 \geq 2$ is an obvious upper bound for C_b^B.

7.2. Application to quadratic fields with $\boldsymbol{n_p = 2}$. We have $g_p = 1$. We obtain $C \approx 0.56402\ldots$ for $10^6 \leq p \leq 10^7$, then $C \approx 0.58341\ldots$ for $10^7 \leq p \leq 10^8$, and $C \approx 0.58326\ldots$ for $10^8 \leq p \leq 10^9$. For larger primes p it seems that the constant C stabilizes. If we replace D by $\phi(D)$ the result is a bit better (e.g., $C \approx 0.64766\ldots$ instead of $0.56402\ldots$ for $10^6 \leq p \leq 10^7$).

The local extremum of C are obtained by primes p, like 166676399, 604929599, 1368987049, 1758415231, for which $p^2 - 1$ is “friable” (product of small primes; see the computations that we shall give in §8.4).

7.3. Application to cyclic cubic fields with $n_p = 3$. We use the program with $g_p = 1$, $n_p = 3$. For instance, for $10^6 \le p \le 10^7$, we get $C \approx 1.5652 \cdots > 1$ as expected from Theorem 6.1; for $10^7 \le p \le 10^8$ the value of C is $1.5399325\ldots$ and for $10^8 \le p \le 3.65717251 \cdot 10^8$, we get $C \approx 1.5809\ldots$.

7.4. Application to quartic fields with $n_p = 2$ and for $n_p = 4$. For $g_p = 2$, $n_p = 2$, and $10^6 \le p \le 10^7$, we get $C = 1.6103\ldots$; for $10^8 \le p \le 10^9$, the result for C is $1.6186\ldots$.

Naturally, for $n_p = 4$ we obtain a larger constant $C = 2.4596\ldots$. But in the case $n_p = 4$ we can test the similar stronger condition $\mathrm{Prob}\,(o_p(\eta) < p^2)$ for which one finds $C = 1.28442\ldots$, giving the conjectural finiteness of totally inert primes p in a Galois quartic field such that $o_p(\eta) < p^2$.

8. Numerical examples with fixed η and $p \to \infty$

The above computations are of a density nature and the upper bound $\frac{1}{p^C}$ is much higher than the true probability. So we intend to take a fixed $\eta \in K^\times$, restrict ourselves to primes p with suitable residue degree n_p, and compute the order of η modulo p to find the solutions p of the inequality $o_p(\eta) < p$.

The programs verify that η generates a multiplicative $\mathbb{Z}[G]$-module of rank n. In the studied cases, $K/\mathbb{Q}$ is Abelian ($G = C_2$, C_3, C_4) and the condition on the rank is equivalent to $\eta^e \ne 1$ in $\langle\eta\rangle_G \otimes \mathbb{Q}$, for all rational idempotents e of $\mathbb{Q}[G]$.

8.1. Cubic cyclic fields. We then consider the following program with the polynomial $P = X^3 + X^2 - 2X - 1$ (see data in Section 3). Put $\eta = ax^2 + bx + c$; then a is fixed and to expect more solutions, b, c vary in $[-10, 10]$ and p in $[3, 10^5]$:

```
{P=x^3+x^2-2*x-1; x0=Mod(x,P); x1=-x0^2-x0+1; x2= x0^2-2;
Borne=10^5; a=1; for(b=-10, 10, for(c=-10, 10,
Eta0=a*x0^2+b*x0+c; Eta1=a*x1^2+b*x1+c; Eta2=a*x2^2+b*x2+c;
N=norm(Eta0); R1=Eta0*Eta1*Eta2; R2=Eta0^2*Eta1^-1*Eta2^-1;
if(R1!=1 & R2 !=1 & R1!=-1 & R2 !=-1,
forprime(p=1, Borne, if(p%N!=0, T=Mod(p,7)^2; if(T!=1,
A=Mod(a,p); B=Mod(b,p); C=Mod(c,p); Y=Mod(A*x^2+B*x+C, P);
my(m=p-1, mm=p^2+p+1); fordiv(m*mm, d, if(d>p, break);
Z=Y^d; if(Z==1, print(a,"  ",b,"  ",c,"  ",p,"  ",d)))))))))}
```

No solution is obtained except the following triples (the eventual multiples of $o_p(\eta)$ are not written):

$$(a, b, c, p, o_p(\eta)) = (1, -7, 7, \mathbf{137}, \mathbf{56}), (1, -3, 3, \mathbf{37}, \mathbf{28}), (1, 4, 8, \mathbf{47}, \mathbf{37}), (1, 6, -10, \mathbf{31}, \mathbf{18}).$$

We have here an example ($\eta = x^2 + 4x + 8$, $p = 47$) where $o_p(\eta) = 37$ divides $p^2 + p + 1 = 37 \cdot 61$; this can be possible because p is too small regarding $\eta^{s^2+s+1} = 1 + 8\,p = 377$ (see Lemma 1.2).

8.2. Quartic cyclic fields. We consider the quartic cyclic field K defined by the polynomial $P = X^4 - X^3 - 6X^2 + X + 1$ of discriminant 34^2. The quadratic subfield of K is $k = \mathbb{Q}(\sqrt{17})$ and $K = k\Big(\sqrt{(17+\sqrt{17})/2}\,\Big)$. The program is analogous to the previous one with the parameters $n_p = g_p = 2$. Put $\eta = ax^3 + bx^2 + cx + d$; then b, c, d vary in $[-10, 10]$, and p in $[3, 10^5]$:

```
{P=x^4-x^3-6*x^2+x+1; x0=Mod(x,P); x1=-1/2*x0^3+3*x0+3/2;
x2=x0^3-x0^2-6*x0+1; x3=-1/2*x0^3+x0^2+2*x0-3/2;
Borne=10^5; a=1; for(b=-10, 10, for(c=-10, 10, for(d=-10, 10,
Eta0=a*x0^3+b*x0^2+c*x0+d; Eta1=a*x1^3+b*x1^2+c*x1+d;
Eta2=a*x2^3+b*x2^2+c*x2+d; Eta3=a*x3^3+b*x3^2+c*x3+d; N=norm(Eta0);
R1=Eta0*Eta1*Eta2*Eta3; R2=Eta0*Eta2^-1; R3=Eta0*Eta1^-1*Eta2*Eta3^-1;
if(R1!=1 & R2 !=1 & R3!=1 & R1!=-1 & R2 !=-1 & R3!=-1,
forprime(p=3, Borne, if(p%N!=0, if(issquare(Mod(p,17))==1,
u=sqrt(Mod(17, p)); v=(17+u)/2; if(issquare(v)==0,
A=Mod(a,p); B=Mod(b,p); C=Mod(c,p); D=Mod(d,p);
Y=Mod(A*x^3+B*x^2+C*x+D,P);
my(m=p-1, mm=p+1); fordiv(m*mm, dd, if(dd>p, break); Z=Y^dd;
if(Z==1, print(a,"  ",b,"  ",c,"  ",d,"  ",p,"  ", dd)))))))))))}
```

No solution is obtained except the following ones, where we consider at most a solution $(p, o_p(\eta))$ for a given p (other solutions may be given by conjugates of η and/or by $\eta' \equiv \eta \pmod p$; many solutions with $p = 19$ and the orders 12 and 15); we eliminate also the solutions $(p, \lambda\, o_p(\eta))$, $\lambda > 1$):

$$
\begin{aligned}
&(a, b, c, d, p, o_p(\eta))\\
&\qquad = (1, -10, 2, -10, \mathbf{19}, \mathbf{12}), (1, -10, 5, -9, \mathbf{19}, \mathbf{15}), (1, -9, 6, 9, \mathbf{43}, \mathbf{33}),\\
&\qquad\quad (1, -7, -2, -6, \mathbf{19}, \mathbf{8}), (1, -7, 2, -8, \mathbf{19}, \mathbf{10}), (1, -8, 7, 7, \mathbf{461}, \mathbf{276}),\\
&\qquad\quad (1, -4, 1, 8, \mathbf{1549}, \mathbf{1395}), (1, -3, 0, -6, \mathbf{223}, \mathbf{64}),\\
&\qquad\quad (1, -1, -6, -10, \mathbf{229}, \mathbf{184}), (1, -1, 3, -2, \mathbf{59}, \mathbf{40}), (1, 3, -8, 6, \mathbf{53}, \mathbf{9}),\\
&\qquad\quad (1, 3, -5, 10, \mathbf{83}, \mathbf{21}), (1, 9, -7, 5, \mathbf{43}, \mathbf{22}).
\end{aligned}
$$

For the last three cases, the order divides $p + 1$ for the same reason as above. We have the more exceptional solution $(1, -4, 1, 8, \mathbf{1549}, \mathbf{1395})$ where $1395 = 9 \cdot 5 \cdot 31$ with $9 \mid p - 1$ and $5 \cdot 31 \mid p + 1$.

8.3. Quadratic fields. We consider the field K defined by the polynomial $P = X^2 - 3$ and the following program with $\eta = a\sqrt{3} + b$, $a = 1$, $b \in [-10, 0]$.

```
{m=3; P=x^2-m; x0=Mod(x,P); x1=-x0; a=1; Borne=10^5;
for(b=-10, 10, Eta0=a*x0+b; Eta1=a*x1+b; N=norm(Eta0);
R1=Eta0*Eta1; R2=Eta0*Eta1^-1; if(R1!=1 & R2 !=1 & R1!=-1 & R2 !=-1,
forprime(p=1, Borne, if(p%N!=0,
```

```
if(kronecker(m, p)==-1, A=Mod(a,p); B=Mod(b,p); Y=Mod(A*x+B,P);
my(m=p-1, mm=p+1); fordiv(m*mm, d, if(d>p, break);
Z=Y^d; if(Z==1, print(a,"  ",b,"  ",p,"  ", d))))))))}
```

For small primes p there are solutions $o_p(\eta) \mid p-1$ or $o_p(\eta) \mid p+1$:

$$\begin{aligned}(a,b,p,o_p(\eta)) \\ &= (1,-10,\mathbf{79},\mathbf{65}),(1,-10,\mathbf{101},\mathbf{75}),(1,-10,\mathbf{967},\mathbf{847}),\\ &\quad (1,-10,\mathbf{20359},\mathbf{13234}),(1,-10,\mathbf{90149},\mathbf{72700}),(1,-9,\mathbf{89},\mathbf{55}),\\ &\quad (1,-9,\mathbf{6163},\mathbf{4623}),(1,-9,\mathbf{29501},\mathbf{6705}),(1,-8,\mathbf{10711},\mathbf{2210}),\\ &\quad (1,-6,\mathbf{1123},\mathbf{843}),(1,-5,\mathbf{86969},\mathbf{81172}),(1,-4,\mathbf{30941},\mathbf{25785}),\\ &\quad (1,-9,\mathbf{41},\mathbf{15}),(1,-9,\mathbf{1301},\mathbf{403}),(1,-8,\mathbf{5},\mathbf{3}),(1,-7,\mathbf{29},\mathbf{24}),\\ &\quad (1,-7,\mathbf{103},\mathbf{39}),(1,-7,\mathbf{727},\mathbf{143}),(1,-4,\mathbf{701},\mathbf{675}),(1,-3,\mathbf{43},\mathbf{33}).\end{aligned}$$

If Conjecture 6.3 is likely for degrees $n \geq 3$, the question arises for quadratic fields with $n_p = 2$. We give here supplementary computations with the following simplified program which can be used changing m, a, b:

```
{m=3; a=5; b=2; Borne=10^9; forprime(p=1, Borne, if(kronecker(m, p)==-1,
A=Mod(a,p); B=Mod(b,p); P=x^2-m; Y=Mod(A*x+B, P);  my(e=kronecker(-4,p));
F1=factor(2*(p-e)); F2=factor((p+e)/2);
P=concat(F1[,1],F2[,1]); E=concat(F1[,2],F2[,2]);
forvec(v=vectorv(# E,i,[0,E[i]]), my(d=factorback(P,v)); if(d>p, next);
Z=Y^d; if(Z==1, print(p,"  ",d)))))}
```

(1) For instance, if we fix $\eta = 5\sqrt{3}+2$ and take larger primes inert in $\mathbb{Q}(\sqrt{3})$, this gives the few solutions (up to $p \leq 10^9$):

$$(p,o_p(\eta)) = (5,4),(29,21),(1063,944),(32707,23384),(90401,68930).$$

(2) For $\eta = 7\sqrt{3}+3$ we obtain the solutions (up to $p \leq 10^9$):

$$(p,o_p(\eta)) = (7,6),(29,21),(137,92),(7498769,5927335),\\ (39208553,31070928).$$

The large solution $(p = 39208553, o_p(\eta) = 31070928)$ (where p^2-1 is friable) is a bad indication for finiteness.

(3) Consider $K = \mathbb{Q}(\sqrt{-1})$ with $p \equiv 3 \pmod 4$ up to $p \leq 10^9$.
- For $\eta = \sqrt{-1}+4$ ($\mathrm{N}(\eta) = 17$), we obtain the solutions:

$$(p,o_p(\eta)) = (49139,19593),(25646167,22440397).$$

- For $\eta = \sqrt{-1}+2$ ($\mathrm{N}(\eta) = 5$), we obtain the solution:

$$(p,o_p(\eta)) = (9384251,6173850).$$

- For $\eta = 3\sqrt{-1} + 11$ ($\mathrm{N}(\eta) = 130$), we obtain the solutions:

$$(p, o_p(\eta)) = (3,2), (43,11), (131,24), (811,174), (911,133), \\ (5743,3168), (2378711,1486695).$$

Although this kind of repartition of the solutions looks like the case of Fermat quotients, for which a specific heuristic can be used (see [3]), it seems that we observe more systematic large solutions in the quadratic case with p inert, and we have possibly infinitely many solutions. This should be because the problem is of a different nature and is connected with generalizations of primitive roots problem in number fields (see the extensive survey by P. Moree [4]).

So we shall try in the next subsection to give some insights in the opposite direction for quadratic fields (infiniteness of inert primes p with $o_p(\eta) < p$).

8.4. Analysis of the quadratic case. Starting from the formula

$$\mathrm{Prob}\,\big(o_p(\eta) < p\big) \le \mathrm{Density}\,\big(o_p(\eta) < p\big) = \frac{1}{p^2-1}\sum_{D\in\mathcal{D}_p}\phi(D)$$

of Remark 6.2 (2), we study the right member of the normalized equality $(p+1)\cdot\mathrm{Density}(o_p(\eta) < p) = \frac{1}{p-1}\sum_{D\in\mathcal{D}_p}\phi(D)$, remembering that it is an upperbound of the probability. From numerical experiments, we can state:

Conjecture 8.1. *Let $\mathcal{D}_p$ be the set of divisors D of p^2-1 such that $D < p$, $D \nmid p-1$, $D \nmid p+1$ (see Theorem 2.1). We have the inequalities:*

$$\frac{1}{3} \le \frac{1}{p-1}\sum_{D\in\mathcal{D}_p}\phi(D) < c(p)\,\log^2(p), \quad p\to\infty,$$

where $c(p)$ is probably around $O(\log_2(p))$.

The majoration $\frac{1}{p^2-1}\sum_{D\in\mathcal{D}_p}\phi(D) < c(p)\cdot\frac{\log^2(p)}{p+1} \sim c(p)\cdot\frac{1}{p^{1-2\cdot\log_2(p)/\log(p)}}$ is to be compared with the upper bound $\frac{1}{p^{1-\varepsilon}}$ (with $\varepsilon = O\big(\frac{1}{\log_2(p)}\big)$) of Theorem 6.1, but the sets of divisors $D \mid p^2-1$ are not the same and this information is only experimental. On the contrary, the minoration

$$\frac{1}{p-1}\sum_{D\in\mathcal{D}_p}\phi(D) \ge \frac{1}{3}$$

seems exact (except very few cases), and although the density ($\ge$ probability) is $\frac{O(1)}{p}$, this suggests the possible infiniteness of inert p such that $o_p(\eta) < p$ for fixed $\eta \in K^\times$ such that η^{1+s} and η^{1-s} are distinct from roots of unity. Indeed, for $p \in \{2,3,5,7,17\}$, we get the strict inverse inequality

$$\frac{1}{p-1}\sum_{D\in\mathcal{D}_p}\phi(D) < \frac{1}{3}$$

and we have no other examples up to 10^9. The equality

$$\frac{1}{p-1}\sum_{D\in\mathcal{D}_p}\phi(D)=\frac{1}{3}$$

is doubtless *equivalent* to $p-1=2^{u+2}\cdot 3^v$ and $p+1=2\cdot\ell$, for some $u\geq 0$, $v\geq 0$ and ℓ prime. To study this, one can use the following programs:

(1) Program testing the equality for any prime p.

```
{b=1; B=10^9; forprime(p=b, B, my(S=0, e=kronecker(-4,p));
F1=factor(2*(p-e)); F2=factor((p+e)/2);
P=concat(F1[,1],F2[,1]); E=concat(F1[,2],F2[,2]);
forvec(v=vectorv(# E,i,[0,E[i]]), my(d=factorback(P,v));
if (d>p, next); if((p-1)%d!=0 && (p+1)%d!=0,
S+= prod(i=1,# v, if(v[i],(P[i]-1)*P[i]^(v[i]-1),1))));
if(3*S==p-1, print(p)))}
```

(2) Program giving the primes p such that $p=1+2^{u+2}\cdot 3^v$ and $p=-1+2\cdot\ell$ (which are trivialy solutions). We use the fact that it is easier to test in first the primality of $(p+1)/2$ for large p.

```
{X=1; Y=1; T=1; J2=0; J3=0; K=0; L=listcreate(10^6);
while(T<10^1000, K=K+1; listput(L,T,K);
if(T==X, J2=J2+1; X=2*component(L,J2));
if(T==Y, J3=J3+1; Y=3*component(L,J3));
T=min(X,Y); p=1+T; if(isprime(p)==1,
my(S=0, e=kronecker(-4,p)); if(isprime((p+1)/2)==1,
F1=factor(2*(p-e)); F2=factor((p+e)/2);
P=concat(F1[,1],F2[,1]); E=concat(F1[,2],F2[,2]);
forvec(v=vectorv(# E,i,[0,E[i]]), my(d=factorback(P,v));
if (d>p, next); if((p-1)%d!=0 && (p+1)%d!=0,
S+= prod(i=1,# v, if(v[i],(P[i]-1)*P[i]^(v[i]-1),1))));
if(3*S==p-1, print(factor(p-1)," ",factor(p+1)," ",p)))))}
```

We obtain the following solutions:

```
p-1              p+1
[2, 2; 3, 1]    [2, 1; 7, 1]     p=13
[2, 2; 3, 2]    [2, 1; 19, 1]     p=37
[2, 3; 3, 2]    [2, 1; 37, 1]     p=73
[2, 6; 3, 1]    [2, 1; 97, 1]     p=193
[2, 7; 3, 2]    [2, 1; 577, 1]     p=1153
[2, 5; 3, 4]    [2, 1; 1297, 1]     p=2593
[2, 2; 3, 6]    [2, 1; 1459, 1]     p=2917
[2, 11; 3, 6]   [2, 1; 746497, 1]     p=1492993
[2, 13; 3, 5]   [2, 1; 995329, 1]     p=1990657
[2, 16; 3, 4]   [2, 1; 2654209, 1]     p=5308417
[2, 20; 3, 3]   [2, 1; 14155777, 1]     p=28311553
[2, 20; 3, 8]   [2, 1; 3439853569, 1]     p=6879707137
[2, 28; 3, 8]   [2, 1; 880602513409, 1]     p=1761205026817
[2, 36; 3, 4]   [2, 1; 2783138807809, 1]     p=5566277615617
[2, 43; 3, 2]   [2, 1; 39582418599937, 1]     p=79164837199873
[2, 47; 3, 3]   [2, 1; 1899956092796929, 1]     p=3799912185593857
```

```
[2, 44; 3, 8]  [2, 1; 57711166318706689, 1]    p=115422332637413377
[2, 19; 3, 26] [2, 1; 666334875701477377, 1]    p=1332669751402954753
[2, 5; 3, 36]  [2, 1; 2401514164751985937, 1]    p=4803028329503971873
[2, 9; 3, 44]  [2, 1; 2521013509590044756175377, 1]    p=5042027019180089512350073
(......)
[2, 347; 3, 210] [2, 1; 224823648231679297678696466529296846133199564204032369510 3
204678086758515245772117788919871231593415601328084363424021522680865363439087937 9
034415848207381872061715069018380030186764812623517632297288335 37, 1]
p=449647296463358595357392933058593692266399128408064739020640935617351703049154 42
355778397424631868312026561687268480430453617307268781758758068831696414763744123 4
30138036760060373529625247035264594576670 73
```

It seems clear that the number of solutions may be infinite (with an exponential growth).

Consider the following program:

```
{b=10^60+floor(Pi*10^35); forprime(p=b, b+10^3, my(S=0, e=kronecker(-4,p));
F1=factor(2*(p-e)); F2=factor((p+e)/2);
P=concat(F1[,1],F2[,1]); E=concat(F1[,2],F2[,2]);
forvec(v=vectorv(# E,i,[0,E[i]]), my(d=factorback(P,v));
if(d>p, next); if((p-1)%d!=0 && (p+1)%d!=0,
S+= prod(i=1,# v, if(v[i], (P[i]-1)*P[i]^(v[i]-1),1))));
Density=S/(p^2-1.0); Delta=S/(p-1.0)-1/3; C= Density*p/log(p);
print(p,"  ", Density,"  ", Delta,"  ",C))}
```

Then we obtain, for the inequalities $\frac{1}{3} \le \frac{1}{p-1}\sum_{D\in\mathcal{D}_p}\phi(D) < c(p)\cdot\log^2(p)$, the following data, showing their great dispersion, first for some small prime numbers, then for some larger ones, where

- Density $:= \frac{1}{p^2-1}\sum_{D\in\mathcal{D}_p}\phi(D)$,
- $\Delta := (p+1)\cdot$ Density $-\frac{1}{3} = \frac{1}{p-1}\sum_{D\in\mathcal{D}_p}\phi(D) - \frac{1}{3}$,
- $C := \frac{p}{\log(p)}\cdot$ Density $\ll c(p)\cdot\log(p)$:

prime number p	Density	Δ	C
112771	1.35×10^{-4}	14.9499	1.3137
112787	3.43×10^{-6}	0.0538	0.0332
112799	1.03×10^{-4}	11.2873	0.9989
112807	2.31×10^{-5}	2.2715	0.2239
112831	3.48×10^{-5}	3.5941	0.3376
112843	9.35×10^{-6}	0.7225	0.0907
100000001234567891011121314151617 2457	3.39×10^{-37}	0.0054	0.0040
1000000012345678910111213141516172551	1.13×10^{-34}	112.7791	1.3645
1000000012345678910111213141516172631	2.02×10^{-35}	19.9470	0.2446
1000000012345678910111213141516172643	9.88×10^{-37}	0.6552	0.0119
1000000012345678910111213141516172661	1.69×10^{-35}	16.5501	0.2036
1000000012345678910111213141516172719	6.83×10^{-35}	67.9646	0.8239
$10^{60}+31415926535897932384626433832795 0343$	1.92×10^{-58}	192.1709	1.3934
$10^{60}+314159265358979323846264338327950499$	1.43×10^{-59}	13.9993	0.1037
$10^{60}+314159265358979323846264338327950541$	5.64×10^{-59}	56.0710	0.4082
$10^{60}+314159265358979323846264338327950569$	7.50×10^{-59}	74.6795	0.5429
$10^{60}+314159265358979323846264338327950989$	2.63×10^{-59}	26.0318	0.1908
$10^{60}+314159265358979323846264338327951201$	5.26×10^{-59}	52.2864	0.3808

(1) For $p = 100000001234567891011121314151617 2457$ above, we have:
$C \approx 0.004086, C/\log(p) \approx 4.930 \cdot 10^{-5}$,
$p - 1 = 2^3 \cdot 3^2 \cdot 389 \cdot 62528362319 \cdot 5710062388314662929 03$,
$p + 1 = 2 \cdot 8131511 \cdot 6148918770113444537621686 4339$.

(2) For $p = 101234567891234567891258 87$, we obtain $\Delta \approx 5.0641 \cdot 10^{-23}$,

$$C \approx 0.005789, C/\log(p) \approx 10.054 \cdot 10^{-5},$$
$$p - 1 = 2 \cdot 50617283945617283945629 43,$$
$$p + 1 = 2^8 \cdot 3 \cdot 131815843608378343608 41.$$

(3) Large values of C are, on the contrary, obtained when $p^2 - 1$ is the product of small primes (friable numbers). This may help to precise the upper bound of C since the local maxima increase slowly. For instance:

$$166676399^2 - 1 = 2^5 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 61$$
$$\text{with } C \approx 41.91845 \text{ and } C/\log(p) \approx 2.21421.$$
$$1758415231^2 - 1 = 2^8 \cdot 3^4 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 29 \cdot 31 \cdot 37 \cdot 47 \cdot 59$$
$$\text{with } C \approx 81.51733 \text{ and } C/\log(p) \approx 3.82932.$$

The following program computes these successive local maxima:

```
{B=10^20; CC=0.0; forprime(p=3, B, my(S=0, e=kronecker(-4,p)); F1=factor(2*(p-e));
F2=factor((p+e)/2); P=concat(F1[,1],F2[,1]); E=concat(F1[,2],F2[,2]);
forvec(v=vectorv(#E,i,[0,E[i]]), my(d=factorback(P,v)); if(d>p, next);
if((p-1)%d!=0 && (p+1)%d!=0, S+= prod(i=1,#v,if(v[i],(P[i]-1)*P[i]^(v[i]-1),1))));
Pr=S/(p^2-1.0); C=Pr*p/log(p); if(C>CC, CC=C; print(p," ",CC," ",CC/log(p))))}

p            CC             CC/log(p)
11           0.1529118768   0.0637692056
19           0.2867929851   0.0974015719
29           0.3690965111   0.1096121427
(......)
604929599   51.9605419985   2.5696806133
1368987049  61.6784084466   2.9318543821
1758415231  81.5173320978   3.8293199014
```

For $p > 1758415231$ the running time becomes prohibitive although we may conjecture the infiniteness of these numbers.

Acknowledgements

Some very fast programs, written in this paper, were suggested by Bill Allombert to obtain the divisors of $p^2 - 1$ and Euler function computations when p is very large. I thank him very warmly for his advices and many improvements of my first “basic” programs.

References

[1] G. Gras, *Class Field Theory: from theory to practice*, corr. 2nd ed., Springer Monographs in Mathematics, Springer, 2005, xiii+507 pages.

[2] ———, "Les θ-régulateurs locaux d'un nombre algébrique : Conjectures p-adiques", *Can. J. Math.* **68** (2016), no. 3, p. 571-624.

[3] ———, "Étude probabiliste des quotients de Fermat", *Funct. Approximatio, Comment. Math.* **54** (2016), no. 1, p. 115-140.

[4] P. Moree, "Artin's Primitive Root Conjecture - A Survey", *Integers* **12** (2012), no. 6, p. 1305-1416.

[5] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer Monographs in Mathematics, Springer, 2004, xi+708 pages.

[6] G. Tenenbaum, *Introduction à la Théorie Analytique et Probabiliste des Nombres*, 4th ed., Belin, 2015, 592 pages.

[7] The PARI Group, "PARI/GP version `2.9.0`", 2016, available from `http://pari.math.u-bordeaux.fr/`.

[8] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics, vol. 83, Springer, 1997, xiv+487 pages.

Georges Gras
Villa la Gardette
chemin Château Gagnière
38520 Le Bourg d'Oisans, France
E-mail: `g.mn.gras@wanadoo.fr`
URL: `http://www.researchgate.net/profile/Georges_Gras`